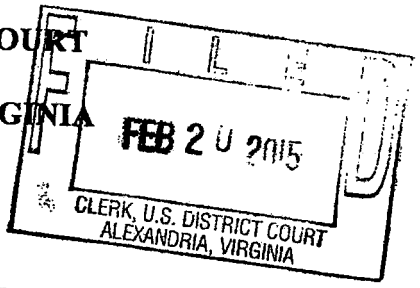
EXHIBIT A

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF COMPUTERS THAT ACCESS upf45jv3bziuctml.onion	)	**FILED UNDER SEAL**
	)	
	)	**Case No. 1:15-SW-89**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Douglas Macfarlane, being first duly sworn, hereby depose and state:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") since April, 1996, and I am currently assigned to the FBI's Violent Crimes Against Children Section, Major Case Coordination Unit ("MCCU"). I currently investigate federal violations concerning child pornography and the sexual exploitation of children and have gained experience through training in seminars, classes, and everyday work related to these types of investigations. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information, in conjunction with criminal investigations pertaining to child pornography the sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

2. I make this affidavit in support of an application for a search warrant to use a network investigative technique ("NIT") to investigate the users and administrators of the website upf45jv3bziuctml.onion (hereinafter "TARGET WEBSITE") as further described in this affidavit and its attachments.[1]

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies as described below; information gathered from the service of subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; my experience, training and background as a Special Agent with the FBI, and communication with computer forensic professionals assisting with the design and implementation of the NIT. This affidavit includes only those facts that I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation.

RELEVANT STATUTES

4. This investigation concerns alleged violations of: 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receiving and Distributing/Conspiracy to Receive and Distribute Child Pornography; and 18 U.S.C. §

[1] The common name of the TARGET WEBSITE is known to law enforcement. The site remains active and disclosure of the name of the site would potentially alert users to the fact that law enforcement action is being taken against the site, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms.

2252A(a)(5)(B) and (b)(2), Knowing Possession, Access or Attempted Access With Intent to View Child Pornography.

a. 18 U.S.C. § 2252A(g) prohibits a person from engaging in a child exploitation enterprise. A person engages in a child exploitation enterprise if the person violates, inter alia, federal child pornography crimes listed in Title 18, Chapter 110, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons;

b. 18 U.S.C. §§ 2251(d)(1) and (e) prohibits a person from knowingly making, printing or publishing, or causing to be made, printed or published, or conspiring to make, print or publish, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

c. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) prohibits a person from knowingly receiving or distributing, or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

d. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

5. The following definitions apply to this Affidavit:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private

messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the bulletin board administrator.

b. "Child erotica," as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.

c. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A "web server," for example, is a

computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital

form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

m. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the Internet Service Provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static,"

if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

n. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

p. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of

any person. See 18 U.S.C. § 2256(2).

q. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

r. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

PROBABLE CAUSE

6. The targets of the investigative technique described herein are the administrators and users of the TARGET WEBSITE - upf45jv3bziuctml.onion - which operates as a "hidden service" located on the Tor network, as further described below. The TARGET WEBSITE is dedicated to the advertisement and distribution of child pornography, the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders use to abuse children, as well as methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes such as those described in paragraph 4 of this affidavit. The administrators and users of the TARGET WEBSITE regularly send and receive illegal child pornography via the website.

The Tor Network

7. The TARGET WEBSITE operates on an anonymity network available to Internet users known as "The Onion Router" or "Tor" network. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of

protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.[2]

8. The Tor software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP back through that Tor exit node IP. In that way, using the Tor network operates similarly to a proxy server – that is, a computer through which communications are routed to obscure a user's true location.

9. Tor also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Tor network itself, entire websites can be set up as "hidden services." "Hidden services,"

2 Users may also access the Tor network through so-called "gateways" on the open Internet such as "onion.to" and "tor2web.org," however, use of those gateways does not provide users with the anonymizing benefits of the Tor network.

like other websites, are hosted on computer servers that communicate through IP addresses and operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

Finding and Accessing the TARGET WEBSITE

10. Because the TARGET WEBSITE is a Tor hidden service, it does not reside on the traditional or "open" Internet. A user may only access the TARGET WEBSITE through the Tor network. Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the site. Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. The TARGET WEBSITE is listed in that section. Accessing the TARGET WEBSITE therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon the TARGET WEBSITE without understanding its

purpose and content. In addition, upon arrival at the TARGET WEBSITE, the user sees images of prepubescent females partially clothed and whose legs are spread with instructions for joining the site before one can enter. Accordingly, there is probable cause to believe that, for the reasons described below, any user who successfully accesses the TARGET WEBSITE has knowingly accessed with intent to view child pornography, or attempted to do so.

Description of the TARGET WEBSITE and Its Content

11. Between September 16, 2014 and February 3, 2015, FBI Special Agents operating in the District of Maryland connected to the Internet via the Tor Browser and accessed the Tor hidden service the TARGET WEBSITE at its then-current Uniform Resource Locator ("URL") muff7i44irws3mwu.onion.[3] The TARGET WEBSITE appeared to be a message board website whose primary purpose is the advertisement and distribution of child pornography. According to statistics posted on the site, the TARGET WEBSITE contained a total of 95,148 posts, 9,333 total topics, and 158,094 total members. The website appeared to have been operating since approximately August 2014 which is when the first post was made on the message board.

12. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to

3 As of February 18, 2015, the URL of the TARGET WEBSITE had changed from muff7i44irws3mwu.onion to upf45jv3bziuctml.onion. I am aware from my training and experience that it is possible for a website to be moved from one URL to another without altering its content or functionality. I am also aware from the instant investigation that the administrator of the TARGET WEBSITE occasionally changes the location and URL of the TARGET WEBSITE in an effort to , in part, avoid law enforcement detection. On February 18, 2015, I accessed the TARGET

the TARGET WEBSITE; and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' (a hyperlink to the registration page) with [TARGET WEBSITE name]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

13. Upon accessing the "register an account" hyperlink, the following message was displayed:

> "VERY IMPORTANT. READ ALL OF THIS PLEASE.
>
> I will add to this as needed.
>
> The software we use for this forum requires that new users enter an email address, and checks that what you enter looks approximately valid. We can't turn this off but the forum operators do NOT want you to enter a real address, just something that matches the xxx@yyy.zzz pattern. No confirmation email will be sent. This board has been intentionally configured so that it WILL NOT SEND EMAIL, EVER. Do not forget your password, you won't be able to recover it.
>
> After you register and login to this forum you will be able to fill out a detailed profile. For your security you should not post information here that can be used to identify you.
>
> Spam, flooding, advertisements, chain letters, pyramid schemes, and solicitations are forbidden on this forum.
>
> Note that it is impossible for the staff or the owners of this forum to confirm the true identity of users or monitor in realtime all messages posted, and as such we are not responsible for the content posted by those users. You remain solely responsible for the content of your posted messages.

WEBSITE in an undercover capacity at its new URL, and determined that its content has not changed.

> The forum software places a cookie, a text file containing bits of information (such as your username and password), in your browser's cache. This is ONLY used to keep you logged in/out. This website is not able to see your IP and can not collect or send any other form of information to your computer except what you expressly upload. For your own security when browsing or Tor we also recomend that you turn off javascript and disable sending of the 'referer' header."

14. After accepting the above terms, registration to the message board then requires a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above. After successfully registering and logging into the site, the following sections, forums, and sub-forums, along with the corresponding number of topics and posts in each, were observed:

Section – Forum	**Topics**	**Posts**	
General Category			
[the TARGET WEBSITE] information and rules		25	236
How to	133	863	
Security & Technology discussion	281	2,035	
Request	650	2,487	
General Discussion	1,390	13,918	
The INDEXES	10	119	
Trash Pen	87	1,273	
[the TARGET WEBSITE] Chan			
Jailbait[4] – Boy	58	154	
Jailbait – Girl	271	2,334	
Preteen – Boy	32	257	
Preteen – Girl	264	3,763	
Jailbait Videos			
Girls	643	8,282	
Boys	34	183	
Jailbait Photos			
Girls	339	2,590	
Boys	6	39	

[4] Based on my training and experience, I know that "jailbait" refers to underage but post-pubescent minors.

Pre-teen Videos		
Girls HC[5]	1,427	20,992
Girls SC/NN	514	5,635
Boys HC	87	1,256
Boys SC/NN	48	193
Pre-teen Photos		
Girls HC	433	5,314
Girls SC/NN	486	4,902
Boys HC	38	330
Boys SC/NN	31	135
Webcams		
Girls	133	2,423
Boys	5	12
Potpourri		
Family [TARGET WEBSITE] – Incest	76	1,718
Toddlers	106	1,336
Artwork	58	314
Kinky Fetish		
Bondage	16	222
Chubby	27	309
Feet	30	218
Panties, nylons, spandex	30	369
Peeing	101	865
Scat	17	232
Spanking	28	251
Vintage	84	878
Voyeur	37	454
Zoo	25	222
Other Languages		
Italiano	34	1,277
Portugues	69	905
Deutsch	66	570
Espanol	168	1,614
Nederlands	18	264
Pyccknn – Russian	8	239

[5] Based on my training and experience, I know that the following abbreviations respectively mean: HC – hardcore, i.e., depictions of penetrative sexually explicit conduct; SC – softcore, i.e., depictions of non-penetrative sexually explicit conduct; NN – non-nude, i.e., depictions of subjects who are fully or partially clothed.

Stories		
Fiction	99	505
Non-fiction	122	675

15. An additional section and forum was also listed in which members could exchange usernames on a Tor-network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

16. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as ".rar" files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

17. A review of the various topics within the "[the TARGET WEBSITE] information and rules," "How to," "General Discussion," and "Security & Technology discussion" forums revealed the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

18. A review of topics within the remaining forums revealed the majority contained discussions, as well as numerous images that appeared to depict child pornography ("CP") and child erotica of prepubescent females, males, and toddlers. Examples of these are as follows:

On February 3, 2015, the user [redacted] posted a topic entitled [redacted] in

the forum "Pre-teen – Videos - Girls HC" that contained numerous images depicting CP of a prepubescent or early pubescent female. One of these images depicted the female being orally penetrated by the penis of a naked male.

On January 30, 2015, the user [redacted] posted a topic entitled [redacted] in the forum "Pre-teen Photos – Girls HC" that contained hundreds of images depicting CP of a prepubescent female. One of these images depicted the female being orally penetrated by the penis of a male.

On September 16, 2014, the user [redacted] posted a topic entitled [redacted] in the "Pre-teen Videos - Girls HC" forum that contained four images depicting CP of a prepubescent female and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent female. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

19. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. Analysis of available historical data seized from the TARGET WEBSITE, as described below, revealed that over 1,500 unique users visited the website daily and over 11,000 unique users visited the website over the course of a week.

20. A private message feature also appeared to be available on the site, after registering, that allowed users to send other users private messages, referred to as "personal messages or PMs," which are only accessible to the sender and recipient of the message. Review of the site demonstrated that the site administrator made a posting on January 28, 2015, in response to another user in which he stated, among other things, "Yes PMs should now be fixed. As far as a limit, I have not deleted one yet and I have a few hundred there now...."

21. Further review revealed numerous additional posts referencing private messages

or PMs regarding topics related to child pornography, including one posted by a user stating, "Yes i can help if you are a teen boy and want to fuck your little sister. write me a private message."

22. Based on my training and experience and the review of the site by law enforcement agents, I believe that the private message function of the site is being used to communicate regarding the dissemination of child pornography and to share information among users that may assist in the identification of the users.

23. The TARGET WEBSITE also includes a feature referred to as "[the TARGET WEBSITE] Image Hosting". This feature of the TARGET WEBSITE allows users of the TARGET WEBSITE to upload links to images of child pornography that are accessible to all registered users of the TARGET WEBSITE. On February 12, 2015, an FBI Agent accessed a post on the TARGET WEBSITE titled [redacted] which was created by the TARGET WEBSITE user [redacted] The post contained links to images stored on "[the TARGET WEBSITE] Image Hosting". The images depicted a prepubescent female in various states of undress. Some images were focused on the nude genitals of a prepubescent female. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent female.

24. The TARGET WEBSITE also includes a feature referred to as "[the TARGET WEBSITE] File Hosting". This feature of the TARGET WEBSITE allows users of the TARGET WEBSITE to upload videos of child pornography that are in turn, only accessible to users of the TARGET WEBSITE. On February 12, 2015, an FBI Agent accessed a post on the TARGET WEBSITE titled [redacted] which was created by the TARGET WEBSITE user [redacted] The post contained a link to a video file stored on "[the TARGET WEBSITE] File

Hosting". The video depicted an adult male masturbating and ejaculating into the mouth of a nude, prepubescent female.

25. The TARGET WEBSITE also includes a feature referred to as "[the TARGET WEBSITE] Chat". On February 6, 2015, an FBI Special Agent operating in the District of Maryland accessed "[the TARGET WEBSITE] Chat" which was hosted on the same URL as the TARGET WEBSITE. The hyperlink to access "[the TARGET WEBSITE] Chat" was located on the main index page of the TARGET WEBSITE. After logging in to [the TARGET WEBSITE] Chat, over 50 users were observed to be logged in to the service. While logged in to [the TARGET WEBSITE] Chat, the following observations were made:

User '[redacted] posted a link to an image that depicted four females performing oral sex on each other. At least two of the females depicted were prepubescent.

User '[redacted] posted a link to an image that depicted a prepubescent female with an amber colored object inserted into her vagina.

User '[redacted] posted a link to an image that depicted two prepubescent females laying on a bed with their legs in the air exposing their nude genitals.

Other images that appeared to depict child pornography were also observed.

26. The images described above, as well as other images, were captured and are maintained as evidence.

THE TARGET WEBSITE SUB-FORUMS

27. While the entirety of the TARGET WEBSITE is dedicated to child pornography, the following sub-forums of the TARGET WEBSITE were reviewed and determined to contain the most egregious examples of child pornography and/or dedicated to retellings of real world

hands on sexual abuse of children.

- Pre-teen Videos - Girls HC
- Pre-teen Videos - Boys HC
- Pre-teen Photos - Girls HC
- Pre-teen Photos - Boys HC
- Potpourri - Toddlers
- Potpourri - Family Play Pen - Incest
- Spanking
- Kinky Fetish - Bondage
- Peeing
- Scat[6]
- Stories - Non-Fiction
- Zoo
- Webcams - Girls
- Webcams - Boys

Identification and Seizure of the Computer Server Hosting the TARGET WEBSITE

28. In December of 2014, a foreign law enforcement agency advised the FBI that it suspected IP address 192.198.81.106, which is a United States-based IP address, to be associated with the TARGET WEBSITE. A publicly available website provided information that the IP Address 192.198.81.106 was owned by [redacted] a server hosting company headquartered at [redacted] Through further investigation, FBI verified that the TARGET

WEBSITE was hosted from the previously referenced IP address. A Search Warrant was obtained and executed at [redacted] in January 2015 and a copy of the server (hereinafter the "TARGET SERVER") that was assigned IP Address 192.198.81.106 was seized. FBI Agents reviewed the contents of the Target Server and observed that it contained a copy of the TARGET WEBSITE. A copy of the TARGET SERVER containing the contents of the TARGET WEBSITE is currently located on a computer server at a government facility in Newington, VA, in the Eastern District of Virginia. Further investigation has identified a resident of Naples, FL, as the suspected administrator of the TARGET WEBSITE, who has administrative control over the computer server in Lenoir, NC, that hosts the TARGET WEBSITE.

29. While possession of the server data will provide important evidence concerning the criminal activity that has occurred on the server and the TARGET WEBSITE, the identities of the administrators and users of the TARGET WEBSITE would remain unknown without use of additional investigative techniques. Sometimes, non-Tor-based websites have IP address logs that can be used to locate and identify the board's users. In such cases, a publicly available lookup would be performed to determine what ISP owned the target IP address, and a subpoena would be sent to that ISP to determine the user to which the IP address was assigned at a given date and time. However, in the case of the TARGET WEBSITE, the logs of member activity will contain only the IP addresses of Tor "exit nodes" utilized by board users. Generally, those IP address logs cannot be used to locate and identify the administrators and users of the TARGET WEBSITE.[7]

30. Accordingly, on February 19, 2015, FBI personnel executed a court-authorized

---

6 Based on my training and experience, "scat" refers to sexually explicit activity involving defecation and/or feces.

7 [redacted] the true IP Addresses of a small number of users of the TARGET WEBSITE (that amounted to less than 1% of registered users

search at the Naples, FL, residence of the suspected administrator of the TARGET WEBSITE. That individual was apprehended and the FBI has assumed administrative control of the TARGET WEBSITE. The TARGET WEBSITE will continue to operate from the government-controlled computer server in Newington, Virginia, on which a copy of TARGET WEBSITE currently resides. These actions will take place for a limited period of time, not to exceed 30 days, in order to locate and identify the administrators and users of TARGET WEBSITE through the deployment of the network investigative technique described below. Such a tactic is necessary in order to locate and apprehend the TARGET SUBJECTS who are engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.

THE NETWORK INVESTIGATIVE TECHNIQUE

31. Based on my training and experience as a Special Agent, as well as the experience of other law enforcement officers and computer forensic professionals involved in this investigation, and based upon all of the facts set forth herein, to my knowledge a network investigative technique ("NIT") such as the one applied for herein consists of a presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location and identity of those users and administrators of the TARGET WEBSITE described in Attachment A who are engaging in the federal offenses enumerated in paragraph 4. Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or "nodes," as described herein, other investigative procedures that are usually employed in criminal investigations of this

---

of the TARGET WEBSITE) were captured in the log files stored on the Centrilogic server.

type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

32. Based on my training, experience, and the investigation described above, I have concluded that using a NIT may help FBI agents locate the administrators and users of the TARGET WEBSITE. Accordingly, I request authority to use the NIT, which will be deployed on the TARGET WEBSITE, while the TARGET WEBSITE operates in the Eastern District of Virginia, to investigate any user or administrator who logs into the TARGET WEBSITE by entering a username and password.[8]

33. In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the TARGET WEBSITE, which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the TARGET WEBSITE, located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

34. The NIT will reveal to the government environmental variables and certain registry-

[8] Although this application and affidavit requests authority to deploy the NIT to investigate any user who logs in to the TARGET WEBSITE with a username and password, in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation, in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users, such as those who have attained a higher status on Website 1 by engaging in substantial posting activity, or in particular areas of TARGET WEBSITE, such as the TARGET WEBSITE sub-

type information that may assist in identifying the user's computer, its location, and the user of the computer, as to which there is probable cause to believe is evidence of violations of the statutes cited in paragraph 4. In particular, the NIT will only reveal to the government the following items, which are also described in Attachment B:

a. The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;

b. A unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating" computers. That unique identifier will be sent with and collected by the NIT;

c. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);

d. Information about whether the NIT has already been delivered to the "activating" computer;

e. The "activating" computer's "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;

f. the "activating" computer's active operating system username; and

g. The "activating" computer's Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the

---

forums described in Paragraph 27.

manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

35. Each of these categories of information described above, and in Attachment B, may constitute evidence of the crimes under investigation, including information that may help to identify the "activating" computer and its user. The actual IP address of a computer that accesses the TARGET WEBSITE can be associated with an ISP and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

36. During the up to thirty day period that the NIT is deployed on the TARGET WEBSITE, which will be located in the Eastern District of Virginia, each time that any user or administrator logs into the TARGET WEBSITE by entering a username and password, this application requests authority for the NIT authorized by this warrant to attempt to cause the user's computer to send the above-described information to a computer controlled by or known to the government that is located in the Eastern District of Virginia.

37. In the normal course of the operation of a web site, a user sends "request data" to the web site in order to access that site. While the TARGET WEBSITE operates at a government

facility, such request data associated with a user's actions on the TARGET WEBSITE will be collected. That data collection is not a function of the NIT. Such request data can be paired with data collected by the NIT, however, in order to attempt to identify a particular user and to determine that particular user's actions on the TARGET WEBSITE.

REQUEST FOR DELAYED NOTICE

38. Rule 41(f)(3) allows for the delay of any notice required by the rule if authorized by statute. 18 U.S.C. § 3103a(b)(1) and (3) allows for any notice to be delayed if "the Court finds reasonable grounds to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in 18 U.S.C. § 2705) . . . ," or where the warrant "provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay." Because there are legitimate law enforcement interests that justify the unannounced use of a NIT, I ask this Court to authorize the proposed use of the NIT without the prior announcement of its use. Announcing the use of the NIT could cause the users or administrators of the TARGET WEBSITE to undertake other measures to conceal their identity, or abandon the use of the TARGET WEBSITE completely, thereby defeating the purpose of the search.

39. The government submits that notice of the use of the NIT, as otherwise required by Federal Rule of Criminal Procedure 41(f), would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing the TARGET WEBSITE. It would, therefore, seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence

of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(1) and 18 U.S.C. § 2705).

40. Furthermore, the investigation has not yet identified an appropriate person to whom such notice can be given. Thus, the government requests authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.

41. The government further submits that, to the extent that use of the NIT can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation. Furthermore, the NIT does not deny the users or administrators access to the TARGET WEBSITE or the possession or use of the information delivered to the computer controlled by or known to the government, nor does the NIT permanently alter any software or programs on the user's computer.

TIMING OF SEIZURE/REVIEW OF INFORMATION

42. Rule 41(e)(2) requires that the warrant command FBI "to execute the warrant within a specified period of time no longer than fourteen days" and to "execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time." After the server hosting the TARGET WEBSITE is seized, it will remain in law enforcement custody. Accordingly, the government requests authority to employ the NIT onto the TARGET WEBSITE at any time of day, within fourteen days of the Court's authorization. The NIT will be used on the TARGET WEBSITE for not more than 30-days from the date of the issuance of the warrant.

43. For the reasons above and further, because users of the TARGET WEBSITE communicate on the board at various hours of the day, including outside the time period between 6:00 a.m. and 10:00 p.m., and because the timing of the user's communication on the board is solely determined by when the user chooses to access the board, rather than by law enforcement, I request authority for the NIT to be employed at any time a user's computer accesses the TARGET WEBSITE, even if that occurs outside the hours of 6:00 a.m. and 10:00 p.m. Further, I seek permission to review information transmitted to a computer controlled by or known to the government, as a result of the NIT, at whatever time of day or night the information is received.

44. The government does not currently know the exact configuration of the computers that may be used to access the TARGET WEBSITE. Variations in configuration, e.g., different operating systems, may require the government to send more than one communication in order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the activating computers for up to 30 days after this warrant is authorized.

45. The Government may, if necessary, seek further authorization from the Court to employ the NIT on the TARGET WEBSITE beyond the 30-day period authorized by this warrant.

SEARCH AUTHORIZATION REQUESTS

46. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

a. the NIT may cause an activating computer – wherever located – to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location,

other information about the computer and the user of the computer, as described above and in Attachment B;

b. the use of multiple communications, without prior announcement, within 30 days from the date this Court issues the requested warrant;

c. that the government may receive and read, at any time of day or night, within 30 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by or known to the government;

d. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an "activating" computer that accessed the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

47. I further request that this application and the related documents be filed under seal. This information to be obtained is relevant to an ongoing investigation. Premature disclosures of this application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of this technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.[9]

[9] The United States considers this technique to be covered by law enforcement privilege. Should the Court wish to

CONCLUSION

48. Based on the information identified above, information provided to me, and my experience and training, I have probable cause to believe there exists evidence, fruits, and instrumentalities of criminal activity related to the sexual exploitation of children on computers that access the TARGET WEBSITE, in violation of 18 U.S.C. §§ 2251 and 2252A.

49. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of these crimes.

50. Based on the information described above, there is probable cause to believe that employing a NIT on the TARGET WEBSITE, to collect information described in Attachment B, will result in the FBI obtaining the evidence and instrumentalities of the child exploitation crimes described above.

Sworn to under the pains and penalties of perjury.

Douglas Macfarlane
Special Agent

Sworn to and subscribed before me
this 20 day of February /s/
Theresa Carroll Buchanan
United States Magistrate Judge
Honorable Theresa Carroll Buchanan
UNITED STATES MAGISTRATE JUDGE

issue any written opinion regarding any aspect of this request, the United States requests notice and an opportunity to be heard with respect to the issue of law enforcement privilege.

ATTACHMENT A

Place to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.

The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL -upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia.

The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;

2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;

3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);

4. information about whether the NIT has already been delivered to the "activating" computer;

5. the "activating" computer's Host Name;

6. the "activating" computer's active operating system username; and

7. the "activating" computer's media access control ("MAC") address;

that is evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and or (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography.

EXHIBIT B

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
OF COMPUTERS THAT ACCESS
upf45jv3bziuctml.onion

Case No. 1:15-SW-89

UNDER SEAL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):
See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 6, 2015
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Honorable Theresa Carroll Buchanan.
(name)

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 2/20/2015 11:45

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Honorable Theresa Carroll Buchanan, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Place to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.

The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL -upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia.

The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;

2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;

3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);

4. information about whether the NIT has already been delivered to the "activating" computer;

5. the "activating" computer's Host Name;

6. the "activating" computer's active operating system username; and

7. the "activating" computer's media access control ("MAC") address;

that is evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and or (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography.

EXHIBIT C

JAP:JMH

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

16M280

– – – – – – – – – – – – – – – – X

UNITED STATES OF AMERICA

- against -

YANG KIM,
also known as "Andrew Kim,"

Defendant.

COMPLAINT

(T. 18, U.S.C. § 2252(a)(2))

– – – – – – – – – – – – – – – – X

EASTERN DISTRICT OF NEW YORK, SS:

JONATHAN B. GERACI, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

On or about and between November 2014 and March 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant YANG KIM, also known as "Andrew Kim," did knowingly receive any visual depiction, the production of such visual depiction having involved the use of one or more minors engaging in sexually explicit conduct and such visual depiction was of such conduct, using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported, by any means including by computer.

(Title 18, United States Code, Section 2252(a)(2)).

The source of your deponent's information and the grounds for his belief are as follows:

1. I have been a Special Agent with the FBI since 2006 and am currently assigned to the New York Office. Since October 2014, I have been assigned to a Crimes Against Children squad and have investigated violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through classroom training and daily work conducting these types of investigations. As a result of my training and experience, I am familiar with the techniques and methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. As part of my responsibilities, I have been involved in the investigation of numerous child pornography ("CP") cases and have reviewed hundreds of photographs and video files depicting minors (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

2. I am familiar with the information contained in this affidavit based on my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution and proliferation of child pornography. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

3. A website ("Website A") was operated on a network ("the Network") available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. Websites that are

accessible only to users within the Network can be set up within the Network and Website A was one such website. Website A could not generally be accessed through the traditional Internet. Only a user who had installed the appropriate software on the user's computer could access Website A.

4. Website A was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting Website A was seized from a web-hosting facility. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to a court order from another federal district court monitored electronic communications of users of Website A.

5. According to data obtained from logs on Website A and monitoring by law enforcement, a user with the user name "zzzzpppp" originally registered an account on Website A on approximately November 14, 2014. Between November 14, 2014, and March 3, 2015, the user "zzzzpppp" actively logged into Website A for a total of approximately 2 hours and 55 minutes.

6. Records obtained for the pertinent time frame show that the IP address used by "zzzzpppp" was registered to an apartment in Queens, New York, within the Eastern District of New York ("the First Apartment"). The investigation further revealed that, subsequent to March 3, 2015, the residents of the First Apartment moved to another apartment in Queens, New York, within the Eastern District of New York ("the Second Apartment").

7. On or about December 22, 2015, along with other FBI Agents, I participated in a voluntary interview of the defendant YANG KIM, also known as "Andrew

Kim," at the Second Apartment. The defendant was advised of the identities of the interviewing agents and the nature of the interview. The defendant was advised that he was not under arrest and that he could discontinue the interview at any time.

8. In sum and substance, the defendant admitted that he began viewing child pornography approximately two and one-half years prior to the interview. He admitted using Website A, and stated that he used the username "zzzzpppp" while doing so.

9. The defendant provided verbal and written consent for the FBI to search his desktop computer, which he stated he had owned for approximately one year. The desktop computer was located in the defendant's room, and the defendant stated that he was the only person who used it.

10. In the course of the search of the defendant's desktop computer, the FBI recovered evidence of multiple video files and image files appearing to depict child pornography. For example, the desktop computer contained, among others, the following video files:

a. **9 yo on hottie on cam finger and orgasm.avi** is a video file that is approximately 11 minutes and 23 seconds in length depicting a young prepubescent female. The young female lays on a bed with her legs spread. The young female then exposes her genitals and digitally penetrates herself.

b. **11 .mp4.mpg** is a video file that is approximately 2 minutes and 40 seconds in length depicting a young prepubescent female. The young female is lying on a bed nude with her legs spread. While her genitals are exposed she is depicted penetrating her genitals with the handle of a hairbrush.

c. **Kansai Chiharu – 14yo!.avi** is a video file that is approximately 1 hour, 13 minutes and 21 seconds which initially depicts a young pubescent female. The video initiates with the young female on a bed. The young female then undresses and lies on a bed nude. An adult male then lays on top of the young female and begins to digitally penetrate her genitals.

The young female then performs oral sex on the adult male followed by the adult male performing oral sex on the young female. The adult male then performs vaginal intercourse with the female her and ejaculates on her genital area. Subsequent scenes include an adult male utilizing a vibrator on the genitals of a young prepubescent female and additional scenes of an adult male engaging in vaginal intercourse with a young pubescent female.

d. **Masha and Veronica Babko 2 (orgasm scenes only).wmv** is a video file that is approximately 16 minutes and 23 seconds in length depicting one young prepubescent female and one young pubescent female. The video initiates with both young females nude and kissing each other. This is followed by each of the females performing oral sex on each other.

WHEREFORE, your deponent respectfully requests that the defendant YANG KIM, also known as "Andrew Kim," be dealt with according to law.

JONATHAN B. GERACI
Special Agent
Federal Bureau of Investigation

Sworn to before me this
23rd day of March, 2016

THE HONORABLE VIKTOR V. POHORELSKY
CHIEF UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

EXHIBIT D

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	No. 3:16-cr-05110-RJB **ORDER ON DEFENDANTS' MOTION TO DISMISS INDICTMENT, DEFENDANTS' MOTION TO SUPPRESS EVIDENCE, DEFENDANTS' MOTION TO EXCLUDE EVIDENCE, AND THIRD ORDER ON DEFENDANTS' MOTION TO COMPEL DISCOVERY**
UNITED STATES OF AMERICA, Plaintiff, v. GERALD LESAN, Defendant.	No. 3:15-cr-00387-RJB **ORDER ON DEFENDANTS' MOTION TO DISMISS INDICTMENT, DEFENDANTS' MOTION TO SUPPRESS EVIDENCE, DEFENDANTS' MOTION TO EXCLUDE EVIDENCE, AND THIRD ORDER ON DEFENDANTS' MOTION TO COMPEL DISCOVERY**
UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	No. 3:15-cr-00274-RJB **ORDER ON DEFENDANTS' MOTION TO DISMISS INDICTMENT, DEFENDANTS' MOTION TO SUPPRESS EVIDENCE, DEFENDANTS' MOTION TO EXCLUDE EVIDENCE, AND THIRD ORDER ON DEFENDANTS' MOTION TO COMPEL DISCOVERY**

THIS MATTER comes before the Court on three motions filed by Defendant David Tippens, Defendant Gerald Lesan, and Defendant Bruce Lorente (collectively, "Defendants"):

(1) Defendants' Motion to Dismiss Indictment (Dkt. 32[1]), (2) Defendants' Motion to Suppress Evidence (Dkt. 35), and (3) Defendants' Motion to Exclude Evidence (Dkt. 31). Also before the Court are unresolved discovery matters of Defendants' Motion to Compel. *See* Dkts. 54, 73, 78, 80, 81, 90. The Court has considered the parties' responsive briefings and supplements thereto (Dkts. 54, 56, 58, 61, 62, 64, 74, 75, 77, 86, 92, 96, 98, 100, 101, 104, 105), evidence and oral argument presented at public hearings held on October 31, 2016 and November 1, 2016 and at an *in camera* hearing held on October 31, 2016 (*see transcript*, Dkts. 102, 103), pleadings filed pursuant to Classified Information Procedures Act (CIPA) 18 U.S.C. App. 3 §§2 and 4 (Dkts. 86, 92, 95), and the remainder of the file herein.[2]

I. BACKGROUND

A. Website A

On February 19, 2015, with the authorization of a warrant issued pursuant to 18 U.S.C. § 2510 *et seq*., the FBI took control of Website A, a website "dedicated" to child pornography, and relocated the site to a government server in Newington, Virginia. The site had more than 100,000 registered member accounts and 1,500 daily visitors. Dkt. 37-1 at ¶¶6, 11, 19. According to an FBI affiant, the homepage, which required users to login to proceed, featured "prepubescent females partially clothed and whose legs are spread with instructions for joining the site before one can enter." *Id*. ¶10. The homepage was changed to feature one youthful female before the warrant was issued, but after the affidavit was prepared.

[1] Docket numbers refer to *United States v. Tippens*, 3:16-cr-05110-RJB, except where otherwise noted. Defendant Lesan and Defendant Lorente filed identical motions, and this order equally pertains to all three cases.
[2] This Court is also assigned *United States v. Michaud*, No. 3:15-5351-RJB (W.D.Wash. 2016), a companion case arising from the same FBI investigation. The presentation in these cases overlap with the showing in *Michaud*, but different and additional presentations have been made here.

After logging in, registered users would view a page with hyperlinks to forum topics, the clear majority of which advertised child pornography. Dkt. 37-1. at ¶¶14-18. Website A operated on the Tor network, a publicly available alternative internet service that allows users to mask identifying information, such as Internet Protocol ("IP") addresses. *Id*. at ¶¶9, 10.

B. The Network Investigating Technique (NIT)

With Website A under its control, on February 20, 2015, the FBI submitted a warrant application to authorize use of a Network Investigating Technology (NIT). Dkt. 37-1. To explain how the NIT works, the Government has offered the declaration and testimony of Dr. Brian Levine. Dkts. 58-1, 102. Defendants have incorporated the declaration of four experts, Vlad Tsyklevich, Matthew Miller, Robert Young, and Shawn Kasal. Dkts. 31-2, 31-3, 31-4, 31-5. Mr. Tsyklevich explained how the NIT works as follows:

> The NIT presented by the FBI works by using an "exploit," a piece of software that takes advantage of a software "vulnerability" in the Tor Browser program. By exploiting this software vulnerability, the NIT is able to circumvent the security protections in the Tor Browser, which under normal circumstances, prevents web sites from determining the true IP address or MAC address of visitors. After exploiting the vulnerability, the NIT delivers a software "payload," a predetermined set of actions, to computers that receive the payload (the "host computer"). The payload used by the FBI in this case collected and then transmitted identifying information about the host computer (including its IP address) along with a unique "identifier" used to associate the target with the identifying information that the NIT collects.

Dkt. 31-2 at ¶4. According to Mr. Tsyklevich, the NIT has four primary components:

> a. Software that generates a payload and injects a unique identifier into it.
>
> b. The "exploit" that is sent to the target computer to take advantage of a software flaw in the Tor Browser.
>
> c. The "payload" that is run on the target computer to extract identifying information about it (such as its IP address).
>
> d. An additional "server component" that stores and preserves the extracted information and allows investigators to access it.

Id.

C. The NIT warrant

The FBI submitted the February 20, 2015 warrant application in the Eastern District of Virginia to Magistrate Judge Theresa Buchanan. According to the warrant application, the NIT causes "activating computers" to "transmit certain information to a computer controlled by or known by the government . . . that may assist in identifying the user's computer, its location, and the user of the computer." Dkt. 37-1 at 33.

The face sheet to the NIT Warrant expressly incorporates two attachments and reads as follows:

> An application by a federal law enforcement officer . . . requests the search of the following person of property located in the ____Eastern___ District of ___Virginia___ (*identify the person or describe the property to be searched and give its location)*:
>
> See Attachment A
>
> The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: See Attachment B[.]

Dkt. 37-2 at 1.

Attachment A reads as follows:

> Attachment A
>
> Place to be Searched
>
> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers below.
>
> The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL – [omitted]— which will be located at a government facility in the Eastern District of Virginia.
>
> The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will

not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

Dkt. 37-2 at 2.

Attachment B reads as follows:

Attachment B

Information to be Seized

From any "activating" computer described in Attachment A:

1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that other "activating" computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the "activating" computer;
5. the "activating" computer's Host Name;
6. the "activating" computer's active operating system username; and
7. the "activating" computer's media access control ("MAC") address;

Dkt. 37-2 at 3.

D. Deployment of the NIT

For approximately 14 days, from February 20, 2015 through March 4, 2015, the FBI administered Website A from a government-controlled computer server located in Virginia, which forwarded a copy of all website communications to FBI personnel in Linthicum, Maryland. Once deployed by the Government, the NIT gathered approximately nine thousand IP addresses, approximately seven thousand of which were associated with computers in one of more than one-hundred countries other than United States. Dkt. 90-1 at 3, 5. The FBI maintains that it did not post content itself, but concedes that it allowed registered users to access the site, view and download child pornographic content for distribution, and post new content,

including 44 "new" series of data. *Id*. at 3. Some website users commented on technical improvements to the site while under FBI control. Dkt. 90-3. A NIT has been relied on by the FBI in at least twenty-three other investigations. Dkt. 100.

E. Local warrants

Based on IP addresses and other identifying information gathered by use of the NIT, officers used databases and other law enforcement tools to develop probable cause to search Defendants' home residences and vehicles. *See generally*, Dkt. 37-3.[3] Warrants were issued by a magistrate judge in the Western District of Washington to search addresses within this district. *Id*. Execution of the local warrants resulted in the seizure of computers and other media devices found to contain child pornography, and allegedly belonging to Defendants.

F. Procedural history and motions

All three defendants are charged in Count I with receipt of child pornography, and in Count II with possession of child pornography. *United States v. Tippens*, 3:16-cr-05110-RJB at Dkt. 15; *United States v. Lesan*, 3:15-cr-000387-RJB at Dkt. 13; *United States v. Lorente*, 3:15-cr-00274-RJB at Dkt. 11. *See* 18 U.S.C. § 2252 (a)(2), (b)(1) (receipt) and (a)(4), (b)(2) (possession).

In Defendants' Motion to Dismiss, Defendants argue that dismissal is warranted based on outrageous government conduct. Dkt. 32.

Defendants' Motion to Suppress challenges the NIT Warrant on two primary grounds: (1) lack of probable cause, and (2) violations of the United States Magistrate Judges Act, 28 U.S.C. § 636, and Fed. R. Crim. P. 41(b). Dkt. 35.

[3] The affidavit cited to is particular only to Defendant Tippens, *see* Dkt. 37-3, but Defendants have consolidated their arguments and make no effort to distinguish one affidavit from another.

In Defendants' Motion to Exclude, Defendants argue that if they are denied the opportunity to review the NIT code in its entirety, the Court should exclude all evidence derived from the NIT code, including evidence found on the computers seized by law enforcement. Dkt. 31. The Government has provided to Defendants "one component of the payload." Dkt. 31-2 at ¶5. At oral argument held on October 31, 2016 and November 1, 2016, the parties agreed that the Government has more recently provided some portions of other components, although the parties have differing views on the significance of the material provided. Dkt. 102 at 11, 12.

To bolster its formal objection to turning over the entire NIT code, the Government requested the opportunity to conduct a CIPA §4 *ex parte, in camera* hearing. Dkt. 86 at 2. The Government also requested the opportunity to explain at that hearing why it should not be required to produce discovery responsive to two discovery requests, Request #5 and Request #8, which were the subject of two prior discovery orders. *Id*. *See* Dkts. 54, 80, 81. The Court granted the request for the CIPA § 4 hearing. Dkt. 95. On October 31, 2016, following the Government's *ex parte* and *in camera* presentation, the Court found that, based on the showing made, the Government was not required to disclose the remaining NIT code or discovery responsive to Request #5 or Request #8. Dkt. 102 at 116.

The Court also granted the Government's request to conduct a CIPA § 2 pretrial hearing. Dkt. 95 at 2. *See* Dkt. 86 at 2. At hearings held on October 31, 2016 and November 1, 2016, Defendants offered no evidence to supplement the written record.

The Government offered to stipulate for trial purposes that an exploit can make changes to security settings that would allow a third party to run commands on a computer without the computer user's knowledge. Dkt. 103 at 65, 66. No stipulation was reached. *Id*. at 71.

II. DISCUSSION

A. Motion to Dismiss (based on outrageous conduct)

It is easy to conclude that the Government acted outrageously here:

(1) The Government ignored the statute forbidding such conduct: "In any criminal proceeding, any property or material that constitutes child pornography . . . shall remain in the care, custody and control of either the Government or the Court." 18 U.S.C § 3509(m).

(2) The Government facilitated the continued availability of Website A, a site containing hundreds of child pornographic images for criminal users around the world.

(3) The Government, in fact, improved Website A's technical functionality.

(4) The Government re-victimized hundreds of children by keeping Website A online.

(5) The Government used the child victims as bait to apprehend viewers of child pornography without informing the victims and without the victims' permission—or that of their families.

(6) The Government's actions placed any lawyer involved in jeopardy for violating ABA Model Rules of Professional Conduct 8.4, and raise serious ethical and moral issues for counsel. *See also*, Washington Rules of Professional Conduct 8.4.

The only justification for the acts of the Government, as provided by counsel, is that the end justifies the means, or in the Government's words, "Because those who create, obtain, trade, distribute and profit from the imagery of the rape and sexual exploitation of children have turned to Tor in an effort to hide their activities, the United States has been forced to

employ creative means to unmask the individuals engaging in the destructive and heinous criminal conduct." Dkt. 101 at 3.

Nevertheless, dismissal of criminal charges due to outrageous conduct by the Government requires consideration of much more than the requisite conduct. "Dismissing an indictment for outrageous conduct . . . is limited to extreme cases in which the defendant can demonstrate that the government's conduct violates fundamental fairness," which is "an extremely high standard." *United States v. Black*, 733 F.3d 294, 302 (9th Cir. 2013) (internal quotations and citations omitted). Under *Black*, "there is no bright line" test to determine whether law enforcement's conduct is outrageous, but the following factors should be considered: (1) known criminal characteristics of the defendants; (2) individualized suspicion of the defendants; (3) the government's role in creating the crime of the conviction; (4) the government's encouragement to commit the offensive conduct; (5) the nature of the government's participation in the offense conduct; and (6) the balance between the nature of the crime and the necessity of the conduct. *Id*. at 303.

> *Black* has provided examples of the types of cases where dismissal is warranted:
>
> It is outrageous for government agents to engineer and direct a criminal enterprise from start to finish . . . to use excessive physical or mental coercion to convince an individual to commit a crime [and] . . . to generate new crimes merely for the sake of pressing criminal charges.

Id. (internal quotations and citations omitted). Conversely, under *Black*, it is not outrageous conduct "to infiltrate a criminal organization, to approach individuals who are already involved in or contemplating a criminal act . . . to provide necessary items to a conspiracy. . . [or] to use artifice and stratagem to ferret out criminal activity." *Id.* at 303 (internal quotations and citations omitted).

Applying the *Black* factors: (1) the Government did not know the criminal characteristics of any defendant; (2) the Government had no individualized suspicion of any defendant; (3) the Government created an opportunity for others to commit the crimes charged, but did not create the crimes charged; (4) the Government did not encourage the crimes charged—only provided the opportunity to persons unknown; (5) the nature of the Government's participation was only to provide an opportunity to commit the crimes charged; and (6) reasonable minds can differ over the balance between the nature—and potential number—of the crimes charged and the necessity for the Governmental conduct, as reflected in the Government's justification for its conduct.

Considering the totality of the circumstances, Defendants have not shown that dismissal based on outrageous government conduct is warranted. Defendants' motion to dismiss should be denied.

B. Motion to Suppress

Defendants' motion to suppress challenges the NIT Warrant in two primary ways: (1) lack of probable cause, and (2) violations of the United States Magistrate Judges Act, 28 U.S.C. § 636, and Fed. R. Crim. P. 41(b).

1. Probable cause

The Fourth Amendment prohibits "unreasonable searches and seizures" and requires that "no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." U.S.Const. Amend. IV. Whether a warrant is supported by probable cause is a totality of the circumstances test that relies on common sense, where the magistrate judge weighs whether there is a "fair probability" that contraband or evidence will be found in a particular place.

United States v. Gourde, 440 F.3d 1065, 1069 (9th Cir. 2006), citing *Illinois v. Gates*, 462 U.S. 213, 214 (1983).

Defendants argue that the NIT Warrant lacks probable cause because it did not describe with particularity how Website A "unabashedly announce[d]" that it was an illegal child pornography site, and that the NIT Warrant amounts to an invalid anticipatory warrant. Dkt. 35 at 27-32. Neither argument is persuasive. First, the FBI affiant provided sufficient detail for a reasonable magistrate judge to conclude that Website A was an illegal child pornography site. The FBI affiant described in detail the homepage, which featured two prepubescent, partially-clothed females, as well as text instructing users how to post photos and video material. Dkt. 37-1 at ¶¶12, 13. The website was not publicly available and could be found only by using a Tor hidden service. *Id*. at ¶¶6-9. The FBI affiant described the items to be gathered by use of the NIT, which, for a period of 30 days, was authorized to be deployed only against registered users of the child pornography site. *Id*. at ¶34. When weighing the totality of the circumstances, the NIT Warrant does not fail for lack of probable cause, especially because the magistrate judge was permitted to rely on the conclusions of the FBI affiant about "where evidence is likely to be found." *United States v. Terry*, 911 F.2d 272, 274 (9th Cir. 1990). *See* Dkt. 37-1 at ¶¶6-37. The fact that the homepage was changed from two prepubescent females to one youthful female between the time that the FBI affidavit was prepared and when the NIT Warrant was issued is immaterial to this conclusion.

Second, although the NIT Warrant may be an anticipatory warrant, as in *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006), the NIT Warrant in this case did not seek to inculpate the "unwitting[], or even passive[]" site visitor. The NIT Warrant was not triggered until a person had logged onto a website with a homepage that prominently displayed an

underage, under-clothed female. Unlike the website in *Gourde*, which could be found with a Google search of a word, "Lolita," *id.*, Website A could not be found by use of a Google search and instead required knowledge of the exact address, which was extremely unlikely to be stumbled on. Dkt. 37-1 at ¶10. The NIT Warrant does not fail for lack of probable cause.

2. 28 U.S.C. § 636

Defendants argue that the NIT Warrant is void because it violated 28 U.S.C. § 636, a violation distinct from the Rule 41(b) violation (discussed below). Dkt. 35 at 2. The United States Magistrates Act, codified at 28 U.S.C. §§ 631-639, provides:

> (a) Each United States magistrate judge . . . shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—
>
> (1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts[.]

28 U.S.C. § 636(a) (emphasis added).

Section 636 and Rule 41(b) have nearly identical language, and § 636 incorporates Rule 41(b), *see* § 636(a)(1), so it is not clear that § 636 violations should be analyzed separately from Rule 41(b) violations. *Compare* § 636 (". . . magistrate judge[s] shall have within the district . . . all powers and duties conferred . . . by the Rules of Criminal Procedure"); *and* Fed. R. Crim. P. 41(b)(1) ("a magistrate judge with authority in the district . . . has authority to issue a warrant to search for . . . property located within the district"). Other courts have unified the analysis, which may be a better way to reconcile the two rules. *See, e.g.,United States v. Broy*, 2016 WL 5172853, at *6 (C.D. Ill. Sept. 21, 2016). Nonetheless, analyzing the NIT Warrant through the lens of § 636, it was lawful for the magistrate judge to authorize deployment of the NIT to search computers within her district, which may have been her intent, but deployment of the NIT resulted in the search of Defendants' computers in the Western District of

Washington and elsewhere, which exceeded the boundaries of the magistrate judge's jurisdiction.

To the extent that the NIT Warrant authorized the search of computers outside of the Eastern District of Virginia, the NIT Warrant violated § 636.

3. Fed. R. Crim. P. 41(b)

Fed. R. Crim. P. 41(b)(1), which has the force of a statute, *see* 18 U.S.C. § 3103, sets out the general rule that "a magistrate with authority in the district . . . has the authority to issue a warrant to search for and seize a person or property located within the district." The rule also carves out exceptions, two of which apply, according to the Government: (1) subdivision (b)(2), where a person or property "might move or be moved outside the district before the warrant is executed," and (2) subdivision (b)(4), which authorizes "install[ing] within the district a tracking device . . . to track the movement of a person located within the district, outside the district, or both[.]" Rule 41(b) is to be applied flexibly, not rigidly, especially as to technology. *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992). In *United States v. New York Tel. Co.*, 434 U.S. 159 (1977), the court noted that a flexible reading of the rule is reinforced by Fed. R. Crim. P. 57(b), which provides that in the absence of controlling law, "a judge may regulate practice in any manner consistent with federal law, these rules and the local rules[.]" *Id.*, at 170.

Rule 41 subdivisions (b)(2) and (b)(4) did not authorize the search of computers in the Western District of Washington or elsewhere beyond the magistrate judge's district. To so interpret those rules appears to stretch their plain language far beyond their intent. Even when flexibly applying the rule, the NIT Warrant violated the letter of Rule 41(b).

Having determined that the NIT Warrant violates Rule 41(b), the next issue is whether the violation was fundamental or technical. "Fundamental errors are those that result in clear constitutional violations," which warrant suppression. *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992) (internal citations omitted). Technical errors warrant suppression only if: (1) there is evidence of deliberate disregard of the rule, or (2) the defendants were prejudiced by the error "in the sense that the search would not have occurred . . . if the rule had been followed or would have been less intrusive absent the error." *Id*.

Defendants argue that a fundamental violation of constitutional magnitude occurred due to the "unprecedented worldwide warrant . . . the cyber equivalent of the general warrants that were anathema to the Founders." Dkt. 74 at 15. The Court previously rejected the lack of particularity argument, finding probable cause for issuance of the NIT Warrant. *See § IIB1 above*. Defendants have not shown that the Rule 41(b) violation was fundamental.

Because the Rule 41(b) violation was not fundamental, it was technical, and suppression is warranted only if there is a requisite showing of deliberate disregard of Rule 41(b) or prejudice. *See United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992). Defendants' argument that the Government acted with deliberate disregard of Rule 41(b) is unavailing. As evidence of deliberate disregard, Defendants point to a Department of Justice letter to the Chair of the Advisory Committee on the Criminal Rules, Dkt. 37-8 at 1, which was sent on September 18, 2013, a date prior to when the FBI sought the NIT Warrant in this case. The DOJ letter proposed changes to Rule 41(b) to "better enable law enforcement to investigate and prosecute botnets and crimes involving Internet anonymizing technologies," because "Rule 41(b) does not directly address the special circumstances that arise . . . where the warrant sufficiently describes the computer to be searched but the district . . . is unknown."

Id. (emphasis added). Defendants' argument would require the Court to make inferences not required by the text of the DOJ letter. The DOJ letter reveals an intent to improve the rule, which does not rule out the possibility that DOJ could have considered Rule 41(b) sufficiently flexible to address changes in technology. *See also*, Dkt. 104-1. Furthermore, the record is silent as to the magistrate judge's thoughts regarding the scope of the warrant at the time it was issued, and speculation on that subject is fruitless. The record does not show deliberate disregard.

Defendants also argue that Defendants were prejudiced, because "if the rule had been heeded . . . [and] the NIT searches . . . properly confined to the Eastern District of Virginia," there would have been no search of Defendants' computers. *Id*. at 10, 11. The definition of prejudice relied upon by Defendants, "in the sense that the search would not have occurred if the rule had been followed," found in *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005), should not be construed broadly. Under Defendants' interpretation, all searches executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter how small or technical the error might be. Tracing the *Weiland* definition to its prior application within the Ninth Circuit, *see United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980), a more workable interpretation of the *Weiland* definition inquires whether evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means, and if so, the defendant did not suffer prejudice.

Applied here, Defendants did not suffer prejudice when they revealed to a third party the key identifying information, their IP addresses, to which they had no reasonable expectation of privacy. *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). As another court within this circuit explained:

> The FBI was ultimately able to locate [the defendant] by tracking his IP address to his internet provider, demonstrating that [the defendant] voluntarily turned his IP address information over to this third party so that it could provide him with web services . . . As [the defendant] does not have an expectation of privacy in his IP address, the FBI could have legally discovered [the defendant's] IP address absent the NIT Warrant.

United States v. Henderson, 15-CR-00565-WHO-1 at 7 (N.D.Cal. Sept. 9, 2016). The fact that Defendants may have attempted to hide their IP addresses does not change the analysis, because the focus is on the reasonableness of, not Defendants' subjective efforts to protect, the expectation of privacy.

The Rule 41(b) violation was technical, not fundamental, and suppression is not warranted based on the violation.

4. Good faith exception

Given the violations of Rule 41(b) and § 636, the next issue is whether the good faith exception bars application of the exclusionary rule. Determining whether to apply the good faith exception to the exclusionary rule where the warrant is issued by a detached and neutral magistrate judge "must be resolved by weighing the costs and benefits of preventing the use . . . of inherently trustworthy tangible evidence . . . that ultimately is found to be defective." *United States v. Leon*, 468 U.S. 897, 906–07 (1984) (internal citations and quotations omitted). Whether a warrant is executed in good faith depends on whether reliance on the warrant was objectively reasonable. If reliance was objectively reasonable, the good faith exception applies, because "excluding the evidence will not further the ends of the exclusionary rule" to deter police misconduct. *Id*. at 918. The determination of whether the good faith exception applies "is an issue separate" from whether constitutional rights were violated by police conduct. *Id*. at 918 (citations and quotations omitted). The exclusionary rule does not apply to deter misconduct of judges or magistrates, because "there exists no evidence suggesting that . . .

lawlessness among [judges and magistrates] actors requires application of the extreme sanction of exclusion." *Id*. at 916.

In this case, reliance on the NIT Warrant was objectively reasonable. The NIT Warrant, issued by a magistrate judge, authorized deploying the NIT from a government-controlled computer server in the Eastern District of Virginia for up to 30 days to search "activating computers." Dkt. 37-2. The NIT Warrant defined "activating computers" as computers of "any user or administrator who logs into [Website A]," from which the FBI was authorized to gather IP addresses and other identifying information. Dkt. 37-2 at 3. The FBI affiant detailed the need for the NIT, based on the nature of Website A, a child pornography site hidden on the Tor network. Dkt. 37-1 at ¶¶9-37. The FBI affiant also described the mechanics of deploying the NIT and the scope of the items to be searched and seized. *Id*. The NIT Warrant authorized solely what was requested by the FBI affiant. Dkt. 37-1 at ¶34; Dkt. 37-2 at 2, 3. Based on these facts, relying on the NIT Warrant was objectively reasonable. The record does not support a finding that the magistrate judge was misled, that the magistrate judge wholly abandoned her role as detached and neutral decisionmaker, that the warrant was issued based on a total lack of probable cause, or other grounds to reject the good faith exception. *See Leon*, 468 U.S. at 923-24.

Defendants argue that the good faith exception should not excuse the Rule 41(b) violation. Dkt. 74 at 24, 25. Under *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992), "[f]undamental errors are those that result in clear constitutional violations . . . [and] require suppression, unless the officers can show good faith reliance as required by *Leon*." *Id*. "To take advantage of *Leon*, the executing agents . . . must demonstrate an objectively reasonable basis for their mistaken belief that the warrant was valid." *Id*. (emphasis

omitted). For technical errors, suppression is required "only if: (1) the defendants were prejudiced by the error, or (2) there is evidence of deliberate disregard of the rule." *Id*. In this case the Rule 41(b) violation was technical, and as previously discussed, there has not been a showing of prejudice or deliberate disregard. Even if the Rule 41(b) violation was fundamental, because reliance was objectively reasonable, the Rule 41(b) violation need not warrant suppression.

Defendants also argue that the good faith exception does not excuse the § 636 violation, Dkt. 74 at 25, but this Court is not aware of any authority that would require exclusion of evidence where officers acted in good faith. Some courts have argued that the *Leon* good faith exception should not extend to the NIT Warrant because the warrant was void *ab initio*. *See, e.g.*, *United States v. Levin*, 2016 WL 2596010, at *10 (D. Mass. May 5, 2016). *Leon* does not make the void *ab initio* distinction urged by Defendants and the court in *Levin*. *Levin* conceded that this is an unresolved area of the law. *Id.* The NIT Warrant was not void *ab initio*, because it was valid at least as to computers within the issuing magistrate judge's district, but even if it was void *ab initio*, § 636 restricts only magistrate judges. The exclusionary rule does not apply to deter the conduct of magistrate judges, who are "neutral judicial officers [who] have no stake in the outcome of particular criminal prosecutions. *Leon*, 468 U.S. at 916-17. *See also*, *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992); *Illinois v. Krull*, 480 U.S. 340, 348 (1987).

The NIT Warrant violated Rule 41(b) and § 636, but because reliance on the warrant was objectively reasonable, the good faith exception bars application of the exclusionary rule. Defendants' motion to suppress should be denied.

C. Motion to Exclude Evidence

Based on the Motion to Exclude (Dkt. 31) and the Motion to Compel Discovery (Dkt. 54), Defendants seek remaining discovery:

> (1) Opportunity to review the NIT code in its entirety;
>
> (2) Request #5: "The names of all agents, contractors, or other personnel who assisted with relocating, maintaining and operating Playpen while it was under Government control"; and
>
> (3) Request #8: "Copies of all correspondence, referrals, and other records indicating whether the exploit . . . has been submitted by the FBI . . . to the White House's Vulnerability Equities Process (VEP) and what, if any, decision was made by the VEP."

Defendants ask the Court for dismissal if the requested discovery is not provided.

While the Government has provided certain information about the NIT to Defendants, it has objected to producing the NIT code in its entirety. The Government requested a CIPA § 4 hearing, which was conducted *ex parte* and *in camera* on the subject of the NIT and the two discovery requests. (The latter were the subjects of prior orders. *See* Dkts. 80, 81.) Following the CIPA § 4 hearing, the Court ruled that it would not compel the Government to produce any of the subject discovery. Also following the CIPA § 4 hearing, the Government suggested a substitute summary of evidence. Defense counsel appeared disinterested in that approach, and no agreement was reached and no order made. 103 at 65, 66, 71. A substitute summary is, however, still available to the parties.

The Court also granted the Government's request to conduct a CIPA § 2 pretrial hearing. Dkt. 95 at 2. *See* Dkt. 86 at 2. CIPA § 2 allows defendants and their attorneys to make admissions not later admissible at trial, 18 U.S.C. App. 3 § 2, but Defendants offered no evidence to supplement the written record.

This state of affairs leads to two issues: (1) whether the withheld material is discoverable under Fed. R. Crim. P. 16, and (2) whether the withheld material is relevant and

helpful to the defense. As discussed below, different standards apply to each issue. If the material is not discoverable, that ends the inquiry. If the discovery is material but not relevant and helpful, that too ends the inquiry. If the evidence is both material and relevant and helpful, the government will have to produce the material or face dismissal.

"Congress passed CIPA to prevent the problem of 'graymail,' where defendants pressed for the release of classified information to force the government to drop the prosecution." *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988). CIPA permits "the trial judge to rule on questions of admissibility involving classified information before introduction of the evidence in open court. . . [which] permits the government to ascertain the potential damage to national security of proceeding with a given prosecution." *Id*. (internal citations omitted). CIPA should not be interpreted to "expand or restrict established principles of discovery . . . [or to] have a substantive impact on the admissibility of probative evidence." *United States v. Sedaghaty*, 728 F.3d 885, 903 (9th Cir. 2013) (internal citations omitted). Instead, CIPA "clarif[ies] the court's powers . . . to deny or restrict discovery in order to protect national security." *Id*. at 904.

CIPA § 2 gives parties the option to move for a pretrial conference "to consider matters relating to classified information that may arise in connection with the prosecution." 18 U.S.C. App. 3 § 2. At this hearing, "the court may consider any matters which relate to classified information or which may promote a fair and expeditious trial," and to that end, "[n]o admission made by the defendant or by any attorney for the defendant . . . may be used against the defendant unless . . . in writing and [] signed[.]" *Id*.

CIPA § 4 provides that the Government may request an *ex parte* hearing to make a showing that, if sufficient, "may authorize the United States to delete specified items of

classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure[.]" 18 U.S.C. App. 3 § 4. That section also authorizes the Government "to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove." *Id.*

Sedaghaty sets out the three-step analysis for CIPA § 4 motions. First, "a district court must first determine whether, pursuant to the Federal Rules of Criminal Procedure, statute, or the common law, the information at issue is discoverable at all." *United States v. Sedaghaty*, 728 F.3d 885, 904 (9th Cir. 2013). Second, the court must "determine whether the government has made a formal claim of the state secrets privilege, lodged by the head of the department which has actual control over the matter, after actual personal consideration by that officer." *Id.* Third, the court must consider whether the evidence is "relevant and helpful to the defense of an accused,'" *id.*, quoting *Roviaro v. United States*, 353 U.S. 53, 60-61 (1957), and if so, "CIPA § 4 empowers the court to determine the terms of discovery, if any." *Id.* (emphasis added).

1. Discoverable?

Under Fed. R. Crim. P. 16(a)(1)(E), the Government is required to produce discovery that is "within the government's possession, custody, or control and . . . is material to preparing the defense." The term "defense" refers to discovery that would "refute the Government's arguments that the defendant committed the crime charged . . . [including] discovery related to the constitutionality of a search or a seizure." *United States v. Soto Zuniga*, __F.3d__ 2016 WL 4932319 (9th Cir. 2016). The NIT code and other requested discovery is discoverable under

Fed. R. Crim. P. 16(a)(1)(E) because of its potential bearing on Defendants' motions, including the constitutional challenges to the NIT Warrant.

2. State secrets privilege?

Based on the Government's filing (Dkt. 86), which invoked a formal claim of privilege, the Court issued a sealed order, the Order Setting [Section 2] Pretrial Conference, Appointing [Classified Information Security Officer], and Granting Leave to File Section 4 Pleading. Dkt. 95. Following the *ex parte* and *in camera* hearing and filings, the Court previously concluded—and now reaffirms its conclusion—that the Government made a sufficient showing to justify withholding the remaining portions of the NIT code and other discovery from Defendants.

3. Relevant and helpful?

There is limited Ninth Circuit case law to guide courts in conducting the *Roviaro* relevant and helpful inquiry, but another District Court in the Ninth Circuit has analyzed the issue at length. *See United States v. Turi*, 143 F.Supp.3d 916, 920 (D.Ariz. 2015). This Court joins the *Turi* court in interpreting "relevant and helpful" to mean that the Government must disclose information—or face dismissal—"only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result . . . would have been different." *Id*. at 921, quoting *Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998). *See also*, *Kyles v. Whitley*, 514 U.S. 419, 436-37 (1995) (right to fair trial not violated "every time the government . . . chooses not to disclose evidence that might prove helpful"). As *Turi* explained, this standard "ensure[s] that a defendant will not be denied a fair trial for national security reasons, while requiring disclosure of classified information only when truly necessary—when the classified information would affect the result of the proceeding." *Id*. To interpret the standard otherwise

would, for all practical purposes, conflate the discoverable inquiry with the relevant and helpful inquiry, depriving the Court of any meaningful discretion to balance the Government's interest in protecting classified national security information with Defendants' interest in accessing pretrial discovery.

The Court is reluctant to make a "relevant and helpful" finding under CIPA § 4. To do so, the Court must attempt to place itself in the shoes of defense counsel and examine the evidence *ex parte* and *in camera* to determine the effect of the evidence on the defense case, if any. Substituting a judge's mind for the fertile minds of defense counsel presents obvious risks to due process and a fair trial. Nevertheless, in rare cases such as this one, it must be done.

At oral argument, Defendants referred to their experts' declarations, which Defendants contend articulate why the Government must produce the entire NIT code. Dkt. 102 at 11; Dkt. 103 at 7, 8, 14-16. The Court now turns to three rationales offered in the declaration of Mr. Tyrklevich, whose declaration is the most detailed of Defendants' four expert declarations, *see* Dkts. 31-2, 31-3, 31-4, 31-5, and a fourth rationale emphasized at oral argument, *see* Dkt. 31-3 at ¶2, to determine whether the full NIT code, and other requested discovery, is relevant and helpful to Defendants.

> *(1) The software that generates a payload and injects a unique identifier into it (component "a") is critical to understanding whether the unique identifier used to link a defendant to access of illegal content is actually unique. If the identifier is generated incorrectly, it could cause different users to be incorrectly linked to each other's actions . . . Without the missing data, I am unable to make a determination about these issues.* Dkt. 31-2 at ¶6 (emphasis added).

Assuming that "different users [were] incorrectly linked to each other other's actions," that would result in the transmission to the FBI of incorrect payload information. Then the unique identifier would not necessarily correspond to the correct IP address or other identifying information. The local search warrants relied on the identifying information, so if incorrect,

this would at worst would result in the search of the wrong home, which would not affect Defendants here. *See United States v. Turner*, 770 F.2d 1508 (9th Cir. 1985) (warrant is sufficiently particular absent a showing of any reasonable probability that another premise might be mistakenly searched); *United States v. Mann*, 389 F.3d 869, 876 (9th Cir. 2004) ("the practical accuracy [of the search warrant] rather than the technical precision governs"). Officers relied on the identifying information in good faith. *C.f. United States v. Collins*, 830 F.2d 145 (9th Cir. 1987) (search of wrong address due to carelessness and lack of common prudence). Furthermore, the search of Defendants' homes was premised not on absolute certainty, but rather on a finding of probable cause, which is a "commonsense, practical question," *United States v. Kelley*, 482 F.3d 1047, 1050 (9th Cir. 2007), and the theoretical possibility of an incorrect unique identifier, which would result in the pursuit of an investigation at the wrong address would not undermine the linchpin of probable cause.

> *(2) . . . Analyzing and understanding the exploit component of the NIT is critical to understanding whether the payload data that has been provided in discovery was the only component executing and reporting information to the government or whether the exploit executed additional functions outside of the scope of the NIT warrant. Without the missing data about the exploit component of the NIT, I am unable to make a determination about these issues.* Dkt. 31-2 at ¶6 (emphasis added).

This rationale theorizes that the NIT, as deployed, may have exceeded the scope of the NIT Warrant as authorized, but Defendants offer nothing to support this theory beyond speculation. A careful review of the affidavits underlying the local warrants shows reliance on the NIT only for identifying information, such as IP addresses, that fall within the scope of the NIT Warrant. *See* Dkt. 37-3 at 79-82, ¶¶28-42. Even if the NIT "executed additional functions" not authorized by the warrant, the remedy would be to suppress unlawfully-gained evidence, not to suppress lawfully-obtained evidence that formed the basis for the local warrants. *See United States v. Payton*, 573 F.3d 859, 864 (9th Cir. 2009).

(3) *In addition, the server component that stores the identifying information returned by the payload (component "d") must faithfully store and reproduce the data it was sent. . . [A]nalyzing this component of the NIT [is] essential to understanding and verifying the digital "chain of custody" of information derived from the NIT. . . [or] I am unable to make a determination about these issues.* Dkt. 31-2 at ¶6 (emphasis added).

This rationale fails even under the assumption that there was an interruption to the "digital chain of custody" between Defendants' computers and the FBI server that stored the information gathered from deployment of the NIT. If there was an interruption, by a hacker, for example, it would at worst corrupt the "identifying information returned by the payload" used to execute local warrants. That would not be fatal to the warrants, especially where officers relied on the identifying information in good faith. *See subsection (1) above.*

The digital chain of custody argument theoretically has more bearing on the charge against Defendants for receipt of child pornography, depending on how the Government elects to show the "knowing receipt" of child pornography. The Government denies the need to rely on any NIT information at trial, but Defendants are justifiably wary of this representation. As to both counts, however, Defendants' argument suffers from the same problem, namely, that Defendants have provided only speculation, not facts, to support their argument.

(4) *Vulnerability to a third party attack that "planted" child pornography on Defendants' computers and compromised computer security settings*. Dkt. 31-3 at ¶2.

Defendants argue that analyzing the remainder of the NIT code, and the exploit in particular, is necessary to determine whether a third party could have accessed Defendants' computers to "plant" the child pornography. Declarations by Defendants' experts contend that this is a real possibility. Dkt. 31-3 at ¶2. However, when pushed by the Government to make a stronger showing beyond arguing that such a third party attack is theoretically possible,

Defendants argued that they are in a "Catch-22" dilemma, because they cannot make a further showing without review of the NIT code that they seek.

Defendants' "apparent Catch-22 is more apparent than real." *United States v. Yunis*, 867 F.2d 617, 624 (D.C. Cir. 1989). Defendants have concededly not conducted forensic investigations of computers seized by law enforcement, and according to the Government, conducting an investigation of the computers, along with the portions of the NIT code already disclosed, would be sufficient to determine third party vulnerability. Defendants insist that they should not need to rely on the Government's representation, but again, Defendants have submitted no factual evidence beyond the theoretical.

For all four rationales raised, but perhaps especially so for the fourth rationale, Defendants' lack of showing is particularly problematic when Defendants had a unique chance for a free bite of the proverbial apple. Under CIPA § 2, Defendants have the chance to make admissions to the Court not admissible against them at trial. *See* 18 U.S.C. App. 3 § 2 ("No admission made by the defendant or by any attorney for the defendant . . . may be used against the defendant unless . . . is in writing and is signed by the defendant and [his] attorney"); FRE 801(d)(2). Defendants did not avail themselves of the opportunity. Such a showing may have moved their argument beyond the theoretical, but the Court is otherwise left with Defendants' mere speculation.

The CIPA § 4 *ex parte* and *in camera* hearing did not reveal any information to persuade the Court that production of the entire NIT would change the probability of a different outcome beyond Defendants' speculation.

The Court finds that disclosing the NIT code in its entirety would not be relevant and helpful to the defense. Although Defendants provide persuasive arguments in the abstract,

upon close examination, and in light of the record provided, Defendants have not shown the reasonable probability of a different outcome if the NIT is produced in its entirety. The remaining NIT code, though discoverable as material under Fed. R. Crim. P. 16(a)(1)(E), is not relevant and helpful to the defense under *Roviaro* and *Sedaghaty* and need not be disclosed to Defendants.

D. Third Order on Defendants' Motion to Compel Discovery

The Court previously found the information requested by Request #5 to be discoverable and the Government's privilege showing to be sufficient (Dkts. 80, 81), so the sole issue as to Request #5 is whether the requested discovery is relevant and helpful. *See United States v. Turi*, 143 F.Supp.3d 916, 920 (D.Ariz. 2015); *Roviaro v. United States*, 353 U.S. 53, 60-61 (1957). The Government's *ex parte* and *in camera* presentation revealed to the Court nothing that would change the probability of a different outcome of dispositive motions or trial. The Court finds that the requested information pertaining to Request #5 is not relevant and helpful to the defense, and its production should not be compelled.

Production of the subject matter of Request #8 should likewise not be compelled. Even if the Court assumes that the requested information is discoverable and that the Government's privilege showing is sufficient, the requested information pertaining to Request #8 is not relevant and helpful to the defense. Production of the requested information should not be compelled.

Not only do Defendants base their request for the NIT information, Request #5, and Request #8 on speculation, but also the Court's examination of the evidence—from the file contents, from public hearings, and from *ex parte* and *in camera* hearings—leads to the conclusion that there is no evidence or information in what the Government may withhold that

would be relevant or helpful to Defendants, that is, there is not a reasonable probability of a different outcome if the material were disclosed to Defendants.

* * *

IV. CONCLUSION

The new technology used to investigate Defendants presents unique constitutional and statutory challenges. As the Court previously noted in *Michaud*, "[t]he Fourth Amendment incorporates a great many specific protections against unreasonable searches and seizures. The contours of these protections in the context of computer searches pose difficult questions." *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006)(internal quotations and citations omitted). The Government's conduct cannot be condoned, but the charges were not dismissible as outrageous. The Government did not violate search and seizure standards enshrined in the United States Constitution. The NIT Warrant violated Rule 41(b) and § 636, but reliance on the warrant was objectively reasonable, and Defendants' speculation about what the remaining NIT code could show does not change the outcome here.

* * *

THEREFORE, it is HEREBY ORDERED:

(1) As to *United States v. Tippens*, 3:16-cr-05110-RJB:

- Defendants' Motion to Dismiss Indictment (Dkt. 32) is DENIED.
- Defendants' Motion to Suppress Evidence (Dkt. 35) is DENIED.
- Defendants' Motion to Exclude Evidence (Dkt. 31) is DENIED.
- Production of the information requested in Defendants' Motion to Compel Discovery in Request #5 and Request #8 (Dkt. 54) shall not be compelled.

(2) As to *United States v. Lesan*, 3:16-cr-00387-RJB:

- Defendants' Motion to Dismiss Indictment (Dkt. 82) is DENIED.
- Defendants' Motion to Suppress Evidence (Dkt. 85) is DENIED.
- Defendants' Motion to Exclude Evidence (Dkt.81) is DENIED.
- Production of the information requested in Defendants' Motion to Compel Discovery in Request #5 and Request #8 (Dkt. 100) shall not be compelled.

(3) As to *United States v. Lorente*, 3:15-cr-00274-RJB:

- Defendants' Motion to Dismiss Indictment (Dkt. 95) is DENIED.
- Defendants' Motion to Suppress Evidence (Dkt.98) is DENIED.
- Defendants' Motion to Exclude Evidence (Dkt.94) is DENIED.
- Production of the information requested in Defendants' Motion to Compel Discovery in Request #5 and Request #8 (Dkt. 113) shall not be compelled.

DONE this 30th day of November, 2016.

ROBERT J. BRYAN
United States District Judge

EXHIBIT E

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
STATESVILLE DIVISION
CASE NO. 5:15-CR-00015-RLV-DCK-1

UNITED STATES,	)	
	)	
	)	
v.	)	
	)	**ORDER**
	)	
STEVEN W. CHASE,	)	
	)	
	)	
	)	

BEFORE THE COURT is a Motion to Dismiss for Outrageous Government Conduct filed by Defendant. (Doc. 80). The Government has filed a response. (Doc. 82). Having fully considered the arguments, evidence, and legal authorities, the Court will **DENY** Defendant's Motion to Dismiss.

I. BACKGROUND

A second superseding indictment alleged that Defendant (1) engaged in a child exploitation enterprise, in violation of 18 U.S.C. § 2252A(g) (2012) (Count 1); (2) conspired to print and publish a notice or advertisement with a visual depiction of child pornography, in violation of 18 U.S.C. § 2251(d), (e) (2012) (Count 2); (3) printed and published a notice or advertisement with a visual depiction of child pornography, in violation of 18 U.S.C. § 2251(d) (Count 3); (4) transported and shipped, by interstate and foreign commerce, material containing child pornography, in violation of 18 U.S.C. § 2252A(a)(1) (Counts 4-6); and (5) possessed material containing an image of child pornography that had traveled in interstate and foreign commerce, in violation of 18 U.S.C. § 2252A(a)(5)(B) (Count 7). (Doc. 31 at 1-4). The charges stem from Defendant's alleged operation of a website. Defendant was arrested on February 20, 2015, the

same day the Federal Bureau of Investigation ("FBI") seized the website and commenced operating the website as part of an ongoing investigation, for which the FBI received judicial authorization. (Doc. 5, Doc. 80-1, Doc. 80-2 at 2, 5-6). During the nearly two weeks that the FBI operated the website, the Government estimates that 100,000 unique users logged into the website, resulting in users making available approximately 9,000 images and 200 videos of pornographic materials featuring children and users posting approximately 13,000 links to other websites that contained pornographic materials featuring children. (Doc. 80-2 at 2-4). In his motion to dismiss, Defendant argues that the Government, by way of the FBI, engaged in outrageous conduct and violated his due process rights by maintaining the website following his arrest.

II. ANALYSIS

Where the government's conduct in the course of a criminal investigation is "so outrageous as to shock the conscience of the court," a defendant may establish a violation of his due process rights. *United States v. Osborne*, 935 F.2d 32, 36 (4th Cir. 1991). The threshold for establishing a due process violation is high and a defendant will not sustain his burden merely by demonstrating "somewhat offensive" or "extremely unsavory" conduct on the part of the government. *Id.*; *see also United States v. Hasan*, 718 F.3d 338, 343 (4th Cir. 2013) (describing a defendant's ability to rely on outrageous government conduct to vacate conviction as theoretical and "highly circumscribed"). Evident of the theoretical nature of a defendant obtaining the dismissal of charges based on outrageous government conduct, neither the United States Court of Appeals for the Fourth Circuit nor the United States Supreme Court have overturned a conviction based on allegedly outrageous government conduct. *See United States v. Russell*, 411 U.S. 423, 430-32 (1973); *Hasan*, 718 F.3d at 343. Furthermore, the plurality opinion in *Hampton v. United States*, 425 U.S. 484, 490 (1976), strongly suggests that a defendant can only establish a due process

violation warranting dismissal of charges based on outrageous government conduct if the conduct deprives the defendant of a specific, protected constitutional right.

Here, the entirety of the investigatory conduct by the FBI on which Defendant relies in support of his motion occurred subsequent to Defendant's arrest for the charged conduct. Therefore, the FBI's operation of the website as part of its ongoing investigation, although arguably unsavory, neither assisted Defendant in allegedly committing the charged acts nor infringed upon any constitutional right belonging to the Defendant.

In an effort to overcome this deficiency in his argument for dismissal, Defendant asserts that the harm to third parties—the children depicted in the 9,000 images, 200 videos, and 13,000 links—during the FBI's operation of the website precludes the Government from relying on the judicial system to prosecute Defendant. Although the case law Defendant cites in support of his argument discusses the possibility that harm to third parties from the investigatory tools employed by the government might present a sufficient ground to reverse a conviction, Defendant fails to cite any case featuring the reversal or dismissal of a conviction based solely on the harm to third parties as a result of the government's investigatory methods. *See United States v. Chin*, 934 F.2d 393, 399-401 (2d Cir. 1991); *United States v. Archer*, 486 F.2d 670, 676-77 (2d Cir. 1973) (conviction reversed on other grounds and possibility of reversal based on harm to third parties left open). Instead, as noted by a plurality of the Supreme Court, in the absence of a constitutional violation, the remedy for "illegal activity" by the police "lies, not in freeing the equally culpable defendant, but in prosecuting the police under the applicable provisions of state or federal law." *Hampton*, 425 U.S. at 490.

IT IS, THEREFORE, ORDERED THAT Defendant's Motion to Dismiss for Outrageous Government Conduct (Doc. 80) be **DENIED.**

Signed: September 6, 2016

Richard L. Voorhees
United States District Judge